L Number	Hits	Search Text	DB	Time stamp
1	2042	713/172-174.ccls. or 713/192-194.ccls. or 713/200.ccls.	USPAT	2004/05/06 10:58
2	1612	380/46.ccls. or 380/28.ccls. or 380/30.ccls.	USPAT	2004/05/06 10:58
3	554	708/100.ccls. or 708/103.ccls. or 708/135.ccls. or 708/250.ccls.	USPAT	2004/05/06 10:59
4	3914	(713/172-174.ccls. or 713/192-194.ccls. or 713/200.ccls.) or (380/46.ccls. or 380/28.ccls. or 380/30.ccls.) or (708/100.ccls. or 708/103.ccls. or 708/135.ccls. or 708/250.ccls.)	USPAT	2004/05/06 10:59
5	9879	(encod$4 or decod$4) and (IC adj2 card or smartcard or token)	USPAT; EPO; JPO; DERWENT	2004/05/06 10:59
6	389	register same ((encod$4 or decod$4)same (IC adj2 card or smartcard or token))	USPAT; EPO; JPO; DERWENT	2004/05/06 10:59
7	2	exponent$4 near2 residual and (RSA or public adj2 key or asymmetric adj2 key)	USPAT; EPO; JPO; DERWENT	2004/05/06 11:00
8	141	modulo adj2 multiplicat$4	USPAT; EPO; JPO; DERWENT	2004/05/06 11:00
9	15433	random near2 number near3 generat$4	USPAT; EPO; JPO; DERWENT	2004/05/06 11:01
10	10087	RSA or public adj2 key or asymmetric adj2 key	USPAT; EPO; JPO; DERWENT	2004/05/06 11:01
11	1395	(RSA or public adj2 key or asymmetric adj2 key) and ((713/172-174.ccls. or 713/192-194.ccls. or 713/200.ccls.) or (380/46.ccls. or 380/28.ccls. or 380/30.ccls.) or (708/100.ccls. or 708/103.ccls. or 708/135.ccls. or 708/250.ccls.))	USPAT; EPO; JPO; DERWENT	2004/05/06 11:01
12	23	((RSA or public adj2 key or asymmetric adj2 key) and ((713/172-174.ccls. or 713/192-194.ccls. or 713/200.ccls.) or (380/46.ccls. or 380/28.ccls. or 380/30.ccls.) or (708/100.ccls. or 708/103.ccls. or 708/135.ccls. or 708/250.ccls.))) and (modulo adj2 multiplicat$4)	USPAT; EPO; JPO; DERWENT	2004/05/06 11:02
13	1395	(RSA or public adj2 key or asymmetric adj2 key) and ((713/172-174.ccls. or 713/192-194.ccls. or 713/200.ccls.) or (380/46.ccls. or 380/28.ccls. or 380/30.ccls.) or (708/100.ccls. or 708/103.ccls. or 708/135.ccls. or 708/250.ccls.))	USPAT; EPO; JPO; DERWENT	2004/05/06 11:02
14	23	((RSA or public adj2 key or asymmetric adj2 key) and ((713/172-174.ccls. or 713/192-194.ccls. or 713/200.ccls.) or (380/46.ccls. or 380/28.ccls. or 380/30.ccls.) or (708/100.ccls. or 708/103.ccls. or 708/135.ccls. or 708/250.ccls.))) and (modulo adj2 multiplicat$4)	USPAT; EPO; JPO; DERWENT	2004/05/06 11:02
15	287	((encod$4 or decod$4) and (IC adj2 card or smartcard or token)) and ((713/172-174.ccls. or 713/192-194.ccls. or 713/200.ccls.) or (380/46.ccls. or 380/28.ccls. or 380/30.ccls.) or (708/100.ccls. or 708/103.ccls. or 708/135.ccls. or 708/250.ccls.))	USPAT; EPO; JPO; DERWENT	2004/05/06 11:02

16	111	(((encod$4 or decod$4) and (IC adj2 card or smartcard or token)) and ((713/172-174.ccls. or 713/192-194.ccls. or 713/200.ccls.) or (380/46.ccls. or 380/28.ccls. or 380/30.ccls.) or (708/100.ccls. or 708/103.ccls. or 708/135.ccls. or 708/250.ccls.))) and (random near2 number near3 generat$4)	USPAT; EPO; JPO; DERWENT	2004/05/06 11:02
17	3	((((encod$4 or decod$4) and (IC adj2 card or smartcard or token)) and ((713/172-174.ccls. or 713/192-194.ccls. or 713/200.ccls.) or (380/46.ccls. or 380/28.ccls. or 380/30.ccls.) or (708/100.ccls. or 708/103.ccls. or 708/135.ccls. or 708/250.ccls.))) and (random near2 number near3 generat$4)) and (modulo adj2 multiplicat$4)	USPAT; EPO; JPO; DERWENT	2004/05/06 11:03
-	1	("5961578").PN.	USPAT	2004/05/05 10:02
-	8658	(encod$4 or decod$4) and (IC adj2 card or smartcard or token)	USPAT	2004/05/06 10:59
-	2209	(encod$4 or decod$4)same (IC adj2 card or smartcard or token)	USPAT	2004/05/05 10:03
-	343	register same ((encod$4 or decod$4)same (IC adj2 card or smartcard or token))	USPAT	2004/05/06 10:59
-	3896	(encod$4 and decod$4) and (IC adj2 card or smartcard or token)	USPAT	2004/05/05 10:04
-	2313	((encod$4 and decod$4) and (IC adj2 card or smartcard or token)) and register	USPAT	2004/05/05 10:16
-	5975	RSA or public adj2 key or asymmetric adj2 key	USPAT	2004/05/06 11:01
-	228	(((encod$4 and decod$4) and (IC adj2 card or smartcard or token)) and register) and (RSA or public adj2 key or asymmetric adj2 key)	USPAT	2004/05/05 10:26
-	0	713/174.ccls. and ((((encod$4 and decod$4) and (IC adj2 card or smartcard or token)) and register) and (RSA or public adj2 key or asymmetric adj2 key))	USPAT	2004/05/05 10:19
-	0	exponential near2 residue and (RSA or public adj2 key or asymmetric adj2 key) and (((encod$4 and decod$4) and (IC adj2 card or smartcard or token)) and register)	USPAT	2004/05/05 10:19
-	343	((encod$4 or decod$4)same (IC adj2 card or smartcard or token)) and (register same ((encod$4 or decod$4)same (IC adj2 card or smartcard or token)))	USPAT	2004/05/05 10:27
-	0	((encod$4 or decod$4)same (IC adj2 card or smartcard or token)) and (register same ((encod$4 or decod$4)same (IC adj2 card or smartcard or token))) and exponent$4 near2 residual	USPAT	2004/05/05 10:28
-	2	exponent$4 near2 residual and (RSA or public adj2 key or asymmetric adj2 key)	USPAT	2004/05/06 11:00
-	0	exponent$4 near2 residual and (IC adj2 card or token or smartcard)	USPAT	2004/05/05 10:32
-	23	exponent$4 near2 residual	USPAT	2004/05/05 13:21
-	13	paul adj2 kocher	USPAT	2004/05/05 13:21
-	11	(paul adj2 kocher) and RSA	USPAT	2004/05/06 08:06
-	88	modulo adj2 multiplicat$4	USPAT	2004/05/06 11:00
-	1	(modulo adj2 multiplicat$4) and ((paul adj2 kocher) and RSA)	USPAT	2004/05/05 14:44
-	88	(modulo adj2 multiplicat$4) or (exponential near2 residue near3 multipli$5)	USPAT	2004/05/05 14:45
-	8022	random near2 number near3 generat$4	USPAT	2004/05/06 11:00

-	5	(paul adj2 kocher) and RSA and (random near2 number near3 generat$4)	USPAT	2004/05/06 08:06
-	69	IC adj2 card same (random near2 number near3 generat$4)	USPAT	2004/05/06 08:07

Google

IC card and RSA and exponentiation   Search   Advanced Search
Preferences

The "AND" operator is unnecessary — we include all search terms by default. [details]

Web   Results **1 - 10** of about **366** for <u>IC **card** and **RSA** and **exponentiation**</u>. (0.45 seconds)

[PDF] <u>Fast Implementation of ESIGN and **RSA** on **IC Cards**
Chung-Huang Yang ...</u>
File Format: PDF/Adobe Acrobat - <u>View as HTML</u>
... few of them considering the **IC card** environment where ... modular
arithmetic algorithms: modular **exponentiation**, modular
multiplication ... of ESIGN and **RSA** algorithms. ...
ccc.ustc.edu.cn/abstract/chyang.pdf - <u>Similar pages</u>

[PDF] <u>Security & Chip **Card** ICs SLE 66CX160S</u>
File Format: PDF/Adobe Acrobat - <u>View as HTML</u>
... It allows fast and efficient calculation of eg **RSA** operations with ...
To minimize the overall power consumption, the chip **card** controller **IC**
offers a ...
www.conseils.fi/SPI_SLE66CX160SU_1001.pdf - <u>Similar pages</u>

[PDF] <u>On the Performance of ESIGN and **RSA** on **IC Cards**</u>
File Format: PDF/Adobe Acrobat - <u>View as HTML</u>
... modular arithmetic algorithms: modular **exponentiation**, modular
multiplication ... implementing ESIGN and **RSA** digital signature ... the
H8/300 general-purpose **IC cards**. ...
www.crypto.idv.tw/publications/scis2003.pdf - <u>Similar pages</u>

[PPT] <u>Some Perspectives on Smart **Card** Cryptography</u>
File Format: Microsoft Powerpoint 97 - <u>View as HTML</u>
... SCIA **IC Card** & System Security Meeting November 16–17, 1998.
... Cryptographic operations in smart **cards** are often accelerated with
coprocessors. ... **RSA** (mod n). ...
www.rsasecurity.com/rsalabs/staff/bios/bkaliski/publications/
other/kaliski-smart-card-crypto-scia-1998.ppt - <u>Similar pages</u>

<u>Microcontrollers suit smart **card** banking applications. ...</u>
... fast modular multiplication, squaring, modular **exponentiation** (with
or without Chinese Remainder Theorem), **RSA** and DSA ... set-top
boxes and **IC card** readers. ...
www.industrialnewsroom.com/fullstory/28256 - 38k - <u>Cached</u> -
<u>Similar pages</u>

[PDF] <u>Security & Chip **Card** ICs SLE 66CX320P</u>
File Format: PDF/Adobe Acrobat - <u>View as HTML</u>
... 273 ms Modular **Exponentiation** using CRT **RSA** Decrypt / **RSA** Signature eq ...
minimize the overall power consumption, the chip **card** controller **IC** offers a ...
www.tu-chemnitz.de/informatik/HomePages/ ThIS/Technik/SLE66CX320P.pdf -
<u>Similar pages</u>

[PDF] <u>Security & Chip **Card** ICs SLE 66CX640P</u>
File Format: PDF/Adobe Acrobat - <u>View as HTML</u>
... ms 273 ms Modular **Exponentiation** using CRT **RSA** Decrypt / **RSA** Signature
Generate ... the overall power consumption, the chip **card** controller **IC** offers a ...
www.infineon.com/ cgi/ecrm.dll/ecrm/scripts/public_download.jsp?
oid=28836&parent_oid=29206 - <u>Similar pages</u>

h   g   g e c   e ch h   e   e   c   e

UltraLock PCI **Cards**
Powered by an UltraLock **IC**, each **card** slides into a standard ... 1K, 2K and 4K-bit **RSA**
key **exponentiation**; PCI v2 ... The first PCI **card** solution we are offering is the ...
www.layern.com/html/ultralock_pci.html - 23k - May 4, 2004 - Cached - Similar pages

[PDF] 15-Series FRAM No.3
File Format: PDF/Adobe Acrobat - View as HTML
... macro only * 3: Size with **exponentiation** excess operation ... Since the **RSA** cipher
involves prime number calculation ... In particular, **IC cards** are expected to be ...
edevice.fujitsu.com/fj/MARCOM/find/21-4e/pdf/89.pdf - Similar pages

[PDF] ECC - The state of the art in smart **card** environments
File Format: PDF/Adobe Acrobat - View as HTML
... 09-23 13 Standard Smart **Card IC** Design EEPROM ... optimized for 512 bit **RSA** −
signature generation ... Fast Accelerator for Modular **Exponentiation**) (1995) • FameX ...

www.cacr.math.uwaterloo.ca/conferences/ 2002/ecc2002/knguyen.pdf - Similar pages

Goooooooooogle ▶
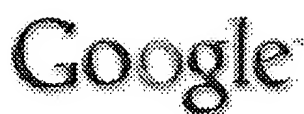
Result Page: 1 2 3 4 5 6 7 8 9 10   **Next**

IC card and RSA and exponentia Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Programs - Business Solutions - About Google

©2004 Google

h   g g e c   e ch h e   e   e   c   e

Web   Images   Groups   News   Froogle^{New!}   more »

IC card and RSA and exponentiation   Search   Advanced Search
Preferences

The "AND" operator is unnecessary -- we include all search terms by default. [details]

Web

Results 11 - 20 of about 366 for **IC card and RSA and exponentiation**. (0.45 seconds)

ST | Industry Leadership on Show at Cartes 96 | T468M

... Already designed into health **cards**, electronic purses, pay TV ... the
industry's most advanced cryptographic smartcard **IC**. ... well as the
basic **RSA** Algorithm functions ...
www.st.com/stonline/press/news/year1996/t468m.htm - 21k - Cached -
Similar pages

ST | STMicroelectronics Receives Common Criteria Level EAL4+ ...

... modular multiplication, squaring, modular **exponentiation** (with
or without Chinese Remainder Theorem), **RSA** and DSA ... was
the first smart **card IC** manufacturer to ...
www.st.com/stonline/press/news/year2002/p1220m.htm - 17k -
Cached - Similar pages

[PDF] Overzicht Informatiebeveiliging "Tekstboek" RSA (1978)

File Format: PDF/Adobe Acrobat - View as HTML
... met private sleutel van CA ESAT- COSIC Motivatie • **RSA** handtekening belet ... op
een digitale handtekening - initialisatie Acquirer POS Device **IC Card** CERT ISS ...
www.esat.kuleuven.ac.be/~preneel/cw03v3.pdf - Similar pages

顏嵩銘

... multi-**exponentiation**計算技術 ... 等，事實上該技術之變化型式亦可 應用於著名之**RSA**
及 ... 上述技術已與相關之**IC card**產業界洽談共 同 ...
www.csie.ncu.edu.tw/~yensm/yensm/Yen-research.htm - 101k - Cached - Similar pages

NemoTech : Smart Card : Glossary Of Terms

... eg variable-length arithmetic, modular **exponentiation** or DES ... **RSA** (Rivest-Shamir-
Adleman) The most widely used ... Smart **Card** Also called **IC card**, chip **card** or ...
www.getoranged.co.za/sc_glossary.php - 53k - May 5, 2004 - Cached - Similar pages

V. 參考文献

... PC Kocher, "Timing Attacks on Implementations of Diffie-Hellman, **RSA**, DSS, and
Other Systems ... Microsoft Smart **Card** of Windows ... 全銀協**IC**カード仕様(改訂版 ...
www.ipa.go.jp/security/fy11/report/contents/ crypto/crypto_report/SmartCard/node65.html
- 15k - Cached - Similar pages

[PDF] www.semiconductors.philips.com/mark ets/identification

File Format: PDF/Adobe Acrobat - View as HTML
... EMV3.1.1 EMV3.1.1 / EMV4.0 EMV3.1.1 EMV3.1.1 Philips' Contact Smart **Card**
Reader ICs ... Std 1k mifare ® Std 4k mifare ® DESFire Product Features MF0 **IC** U1X
MF1 ...
www.semiconductors.philips.com/acrobat/ literature/9397/75011276.pdf - Similar pages

BYTE.com

... More elaborate functions such as **RSA** signatures and ... health **cards**, Stored-value
cards, health **cards**, pay TV ... The ST19 smartcard **IC** has on-chip security functions ...
www.byte.com/art/9706/sec4/art4.htm - 23k - Cached - Similar pages

[PDF] **EDITORIAL**
File Format: PDF/Adobe Acrobat - <u>View as HTML</u>
... to a data string prior to applying the **RSA exponentiation** operation. ... Pryds
Pedersen Personaliser Issuer Secure Storage Public Key **IC Card** personalisation data ...

www.cryptomathic.com/pdf/news1.pdf - <u>Similar pages</u>

rsa beta - iaik
... Although multiplication and **exponentiation** algorithms exist that have ... reduce the
computational effort of **RSA** encryption by ... external clock of the **IC** tester and ...
www.iaik.tu-graz.ac.at/research/vlsi%20design/ high%20speed%20rsa/rsa%
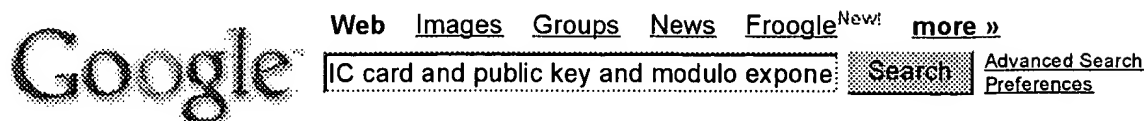20beta/index.php - 16k - <u>Cached</u> - <u>Similar pages</u>

◀ Gooooooooooogle ▶

Result Page: **Previous** <u>1</u> <u>2</u> <u>3</u> <u>4</u> <u>5</u> <u>6</u> <u>7</u> <u>8</u> <u>9</u> <u>10</u><u>11</u>   **Next**

| IC card and RSA and exponentia | Search |

<u>Search within results</u> | <u>Language Tools</u> | <u>Search Tips</u>

<u>Google Home</u> - <u>Advertising Programs</u> - <u>Business Solutions</u> - <u>About Google</u>

©2004 Google

h   g g e c   e ch   c   e   e   h e   e

Web   Images   Groups   News   Froogle^{New!}   **more »**

Google

| IC card and public key and modulo expone: | Search | Advanced Search
Preferences |

The "AND" operator is unnecessary – we include all search terms by default. [details]

Web   Results **1 - 10** of about **606** for <u>**IC** card and public **key** and **modulo** exponentiation</u>. (0.31 seconds)

[PPT] <u>Some Perspectives on Smart **Card** Cryptography</u>
File Format: Microsoft Powerpoint 97 - <u>View as HTML</u>
... SCIA **IC Card** & System Security Meeting November 16 ... Handschuh and P. Paillier, "Smart
Card Crypto-Coprocessors for **Public-Key** Cryptography," RSA ...
www.rsasecurity.com/rsalabs/staff/bios/bkaliski/publications/ other/kaliski-smart-card-crypto-scia-1998.ppt -
<u>Similar pages</u>

[PDF] <u>Fast Implementation of ESIGN and RSA on **IC Cards** Chung-Huang Yang ...</u>
File Format: PDF/Adobe Acrobat - <u>View as HTML</u>
... unsuitable for **public-key** cryptosystems or ... considering the **IC card** environment where ... arithmetic
algorithms: **modular exponentiation**, **modular** multiplication, and ...
ccc.ustc.edu.cn/abstract/chyang.pdf - <u>Similar pages</u>

<u>BYTE.com</u>
... generator, the ST19 can perform full **public-key** generation, digital ... **cards**, Stored-value
cards, health **cards**, pay TV ... The ST19 smartcard **IC** has on-chip security ...
www.byte.com/art/9706/sec4/art4.htm - 23k - <u>Cached</u> - <u>Similar pages</u>

[PDF] <u>ECC - The state of the art in smart **card** environments</u>
File Format: PDF/Adobe Acrobat - <u>View as HTML</u>
... 09-23 13 Standard Smart **Card IC** Design EEPROM RAM ... Fame (Fast Accelerator for **Modular
Exponentiation**) (1995) • FameX ... usage for other **Public Key** Crypto systems ...
www.cacr.math.uwaterloo.ca/conferences/ 2002/ecc2002/knguyen.pdf - <u>Similar pages</u>

[PDF] <u>Security & Chip **Card** ICs SLE 66CX160S</u>
File Format: PDF/Adobe Acrobat - <u>View as HTML</u>
... 700 bytes and supports all of today known **public-key** algorithms based ... minimize the
overall power consumption, the chip **card** controller **IC** offers a ...
www.conseils.fi/SPI_SLE66CX160SU_1001.pdf - <u>Similar pages</u>

<u>Microcontrollers suit smart **card** banking applications. ...</u>
... plus on-chip library support for asymmetrical (**public key**) algorithms ... technology and
its products play a **key** role in ... Chip suits set-top boxes and **IC card** readers ...
www.industrialnewsroom.com/fullstory/28256 - 38k - <u>Cached</u> - <u>Similar pages</u>

<u>Philips Semiconductors - News - Philips Semiconductors' high ...</u>
... flexibility in choosing and implementing specific **public key** algorithms ... the highest
execution speed of any smartcard **IC** in production: **card** manufacturers can ...
www.semiconductors.philips.com/ news/content/file_316.html - 31k - <u>Cached</u> - <u>Similar pages</u>

<u>Philips Semiconductors - News - Philips Semiconductors announces ...</u>
... the world's first smart **card** cryptocontroller **IC** family based ... the platform for smart
card cryptocontrollers on ... as well as different **public key** algorithms based ...
www.semiconductors.philips.com/ news/content/file_356.html - 30k - <u>Cached</u> - <u>Similar pages</u>
[<u>More results from www.semiconductors.philips.com</u>]

<u>ST | STMicroelectronics Receives Common Criteria Level EAL4+ ...</u>
... cryptographic library of firmware routines that support **Public Key** Cryptography with

h   g   g e c   e   ch   c   b c e   e   e   b

key lengths up ... ST was the first smart **card IC** manufacturer to ...
www.st.com/stonline/press/news/year2002/p1220m.htm - 17k - Cached - Similar pages

[PDF] Dynamic Authentication of Smart **Cards** without Crypto-Processor
File Format: PDF/Adobe Acrobat - View as HTML
... **Card IC** Terminal Communication between **IC Card** and Terminal ... Louis Guillou, FT R&D,
Smart **Card** Seminar, Singapour ... signature of Id when the **public exponent** v is ...
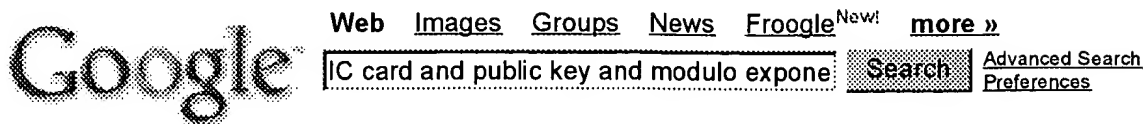www.itsc.org.sg/standards_news/2002-12/guillou-gq2.pdf - Similar pages

Gooooooooogle ▶

Result Page: 1 2 3 4 5 6 7 8 9 10   **Next**

| IC card and public key and modu | Search |

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Programs - Business Solutions - About Google

©2004 Google

h   g g e c   e ch   c   b c e   e   e   b

Web   Images   Groups   News   Froogle[New!]   **more »**

| IC card and public key and modulo expone | Search | Advanced Search |
| | | Preferences |

The "AND" operator is unnecessary — we include all search terms by default. [details]

Web   Results **11 - 20** of about **606** for **IC card and public key and modulo exponentiation**. (0.33 seconds)

ST | Industry Leadership on Show at Cartes 96 | T468M
... Already designed into health **cards**, electronic purses ... is the industry's most advanced
cryptographic smartcard **IC**. ... required for popular **Public Key** algorithms to ...
www.st.com/stonline/press/news/year1996/t468m.htm - 21k - Cached - Similar pages
[More results from www.st.com]

[PDF] Rubicon Data Sheet
File Format: PDF/Adobe Acrobat - View as HTML
... consumption 5W • E-commerce Servers o PCI **cards** o Motherboards o ... CS 1 0 1 5 / Rub
ic on PCI ... asymmetric **key** processor performs the critical **public**/private **key** ...
www.chipsign.com/ downloads/CS1015_Product_Brief_102.pdf - Similar pages

[PDF] Overzicht Informatiebeveiliging "Tekstboek" RSA (1978)
File Format: PDF/Adobe Acrobat - View as HTML
... P **IC** Private **Key Public Key** Static **Card** data CERT ... and Sign Transaction with S **IC** Source:
Mastercard ... an encrypted pre - secret Pre- Secret **Public Key** D Private ...
www.esat.kuleuven.ac.be/~preneel/cw03v3.pdf - Similar pages

V. 参考文献
... A Method for Obtaining Digital Signatures and **Public-key** Cryptosystems", Communications ... Microsoft
Smart **Card** of Windows ... 全銀協ICカード仕様(改訂版 ...
www.ipa.go.jp/security/fy11/report/contents/ crypto/crypto/report/SmartCard/node65.html - 15k - Cached -
Similar pages

[PDF] Security & Chip Card ICs SLE 66CX320P
File Format: PDF/Adobe Acrobat - View as HTML
... To minimize the overall power consumption, the chip **card** controller **IC** offers a ... bytes
and supports all of today known **public-key** algorithms based on ...
www.tu-chemnitz.de/informatik/HomePages/ ThIS/Technik/SLE66CX320P.pdf - Similar pages

SRAM-Based Microcontroller Optimizes Security
... perimeter, but remote payment terminals in **public** places are ... as ISO-7816- compliant
smart-**card** readers, fingerprint ... can be used for secret **key** storage, data ...
www.maxim-ic.com/appnotes.cfm/appnote_number/2033 - 39k - Cached - Similar pages

Smart Card Glossary
... Visa **IC Card** Specification: the scheme which governs chip **card** ... Microsoft's multi-application
card platform (cf ... tests make use of **public key** cryptography, where ...
home.btclick.com/mhendry/glossary.htm - 69k - Cached - Similar pages

Citations: Digitalized signatures and public-key functions as ...
... taking f to be the **modular** squaring function ... Rabin, Digitalized signatures and **public-key**
functions as ... Integrated Circuit **Card** Specification for Payment Systems ...
citeseer.ist.psu.edu/context/36368/0 - 37k - Cached - Similar pages

Hardware architectures for public key cryptography
... Information Security Workshop on Smart **Cards**: Technology, Applications ... AG, SLE 66CUX640P:
USB Security **IC**, St. ... E. Hess, Aspects of **public key** cryptosystems in ...

h   g gec   e ch   c   b c e   e   e   h

portal.acm.org/ citation.cfm?id=861066&dl=ACM&coll=portal&CFID=11111111&CFTOKEN=2222222 - Similar pages

[PDF] System LSIs with Cryptographic Functions and Their Applications
File Format: PDF/Adobe Acrobat - View as HTML
... a central processing unit (CPU) on an **IC** chip can ... of the H8/3113 smart- **card** microcomputer developed ... the de facto world standard in **public-key** cryptography, at ...
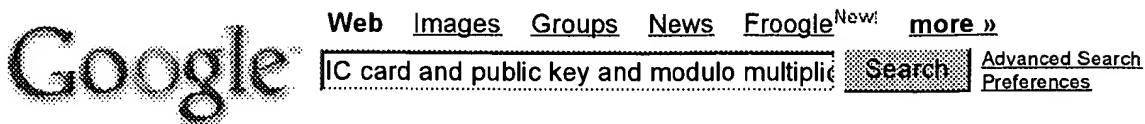www.hitachi.com/rev/1999/revdec99/R6-110-final.pdf - Similar pages

◀ Gooooooooooogle ▶

Result Page: **Previous** 1 2 3 4 5 6 7 8 9 10 11   **Next**

IC card and public key and modu   Search

Search within results | Language Tools | Search Tips

Google Home - Advertising Programs - Business Solutions - About Google

©2004 Google

h   g g e c   e ch   c   b c e   e   e   h

Web   Images   Groups   News   Froogle^{New!}   more »

Google

IC card and public key and modulo multiplic [Search]   Advanced Search
Preferences

The "AND" operator is unnecessary – we include all search terms by default. [details]

Web   Results **1** - **10** of about **727** for <u>IC card and public key and modulo multiplication</u>. (0.47 seconds)

[PDF] <u>Fast Implementation of ESIGN and RSA on IC Cards</u>
<u>Chung-Huang Yang ...</u>
File Format: PDF/Adobe Acrobat - <u>View as HTML</u>
... traditionally unsuitable for **public-key** cryptosystems or ...
considering the **IC card** environment where ... **modular** exponentiation,
modular multiplication, and **modular ...**
ccc.ustc.edu.cn/abstract/chyang.pdf - <u>Similar pages</u>

<u>iccard_AG</u>
... part for high security application in **Public key** Infrastucture. ... RSA
encryption in a tiny smart **card**, a co ... Thus, **IC card** OS Evaluation
System provides a secure ...
www.hmsa.hitachi.com.hk/focus_ap/ic_card/dsa1024.htm - 26k -
<u>Cached</u> - <u>Similar pages</u>

[PDF] **IC CARD EVALUATION SYSTEM: DSA-COS & PC S/W**
File Format: PDF/Adobe Acrobat - <u>View as HTML</u>
... System Part No • K-DSA-COSPC **IC CARD** EVALUATION SYSTEM ... parts for high
security application in **Public Key** Infrastructure. ... encryption in a tiny smart **card**, a
co ...
www.hmsa.hitachi.com.hk/focus_ap/ic_card/dsa_cos.pdf - <u>Similar pages</u>

[PDF] <u>Design of High Speed Long Calculation Units for **Public-Key** ...</u>
File Format: PDF/Adobe Acrobat
... its dominant role Increasing interest in **public key** schemes based ... Security & Chip
Card ICs What is "**modular ...** $c \equiv a+b \bmod N$ **Modular multiplication**: Find the ...
www.nmda.or.jp/nmda/ic-card/proceedings/ 30-1030-Seifert.pdf - <u>Similar pages</u>

<u>Microcontrollers suit smart **card** banking applications. ...</u>
... plus on-chip library support for asymmetrical (**public key**) algorithms ... technology
and its products play a **key** role in ... Chip suits set-top boxes and **IC card** readers ...
www.industrialnewsroom.com/fullstory/28256 - 38k - <u>Cached</u> - <u>Similar pages</u>

<u>BYTE.com</u>
... generator, the ST19 can perform full **public-key** generation, digital ... **cards**, Stored-
value **cards**, health **cards**, pay TV ... The ST19 smartcard **IC** has on-chip security ...
www.byte.com/art/9706/sec4/art4.htm - 23k - <u>Cached</u> - <u>Similar pages</u>

[PDF] <u>ECC - The state of the art in smart **card** environments</u>
File Format: PDF/Adobe Acrobat - <u>View as HTML</u>
... r,s), hash h: base point P, **public key** Q=dP ... 2002-09-23 13 Standard Smart **Card IC**
Design EEPROM ... **multiplication**, uses the fact the reduction **modulo** perfect
powers ...
www.cacr.math.uwaterloo.ca/conferences/ 2002/ecc2002/knguyen.pdf - <u>Similar pages</u>

<u>ST | STMicroelectronics Receives Common Criteria Level EAL4+ ...</u>
... cryptographic library of firmware routines that support **Public Key** Cryptography with
key lengths up ... ST was the first smart **card IC** manufacturer to ...
www.st.com/stonline/press/news/year2002/p1220m.htm - 17k - <u>Cached</u> - <u>Similar pages</u>

Chung-Huang Yang
... Chung-Huang Yang, "**Modular** Arithmetic Algorithms for Smart ... Yang, "Campus Smart **Cards** with **Public-Key** Infrastructure, " TANET ... of ESIGN and RSA on **IC Cards**," Proc ...
crypto.nknu.edu.tw/psnl/vita.htm - 65k - Cached - Similar pages

Searching for post-doctoral researchers *** (Please re-distribute ...
... open platform for **IC cards**), application and ... issues for **public key** cryptography (including exponentiation, **modular multiplication**, and others ...
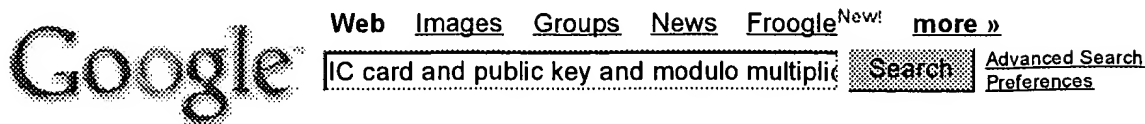www.csie.ncu.edu.tw/~yensm/event/postdoct.txt - 6k - Cached - Similar pages

Goooooooooogle ▶

IC card and public key and modu Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Programs - Business Solutions - About Google

h   g g e c   e ch   c   b c e   c   b

Google

IC card and public key and modulo multipli | Search | Advanced Search / Preferences

The "AND" operator is unnecessary – we include all search terms by default. [details]

Web   Results **11** - **20** of about **727** for **IC card and public key and modulo multiplication**. (0.37 seconds)

Hardware architectures for **public key** cryptography
... Security Workshop on Smart **Cards**: Technology, Applications ... AG,
SLE 66CUX640P: USB Security **IC**, St. ... Fast arithmetic architectures
for **public-key** algorithms over ...
portal.acm.org/ citation.cfm?
id=861066&dl=ACM&coll=portal&CFID=11111111&CFTOKEN=2222222
- Similar pages

[PDF] Hardware für Kryptographische Anwendungen (Seminar) ...
File Format: PDF/Adobe Acrobat - View as HTML
... Rucksack) Verfahren • A. Salomaa: **Public -Key** Cryptography, 2 ...
Applications on a Smart **Card IC**", pp ... of Montgomery's **Modular
Multiplication** Algorithm; IEEE ...
informatik.uibk.ac.at/~c70236/2003ws/lit.pdf - Similar pages

[PDF] Checking Before Output May Not Be Enough Against Fault-Based ...
File Format: PDF/Adobe Acrobat - View as HTML
... as A e mod N , where e is the **public key** corresponding to ... to notice that the clock
signal of current smart **IC cards** is supplied from the **card** reader. ...
www.gemplus.com/smart/r_d/publications/ pdf/YJ00chkb.pdf - Similar pages

[PS] Checking Before Output May Not Be Enough
File Format: Adobe PostScript - View as Text
... as Ae mod N , where e is the **public key** corresponding to ... to notice that the clock
signal of current smart **IC** cardsis supplied from the **card** reader. ...
www.gemplus.com/smart/r_d/publications/ps/YJ00chkb.ps - Similar pages

[PDF] Introduction Montgomery **Multiplication** Algorithm
File Format: PDF/Adobe Acrobat - View as HTML
... time The time to calculate a **modular** exponentiation is ... low hardware cost such as
IC cards References R ... On digital signatures and **public key** cryptosystems Comm ...
dove.kornu.ac.kr/~jcha/paper/jwisc_form2.pdf - Similar pages

Citations: Digitalized signatures and **public-key** functions as ...
... taking f to be the **modular** squaring function ... Rabin, Digitalized signatures and
public-key functions as ... Integrated Circuit **Card** Specification for Payment Systems ...
citeseer.ist.psu.edu/context/36368/0 - 37k - Cached - Similar pages

Body
... 2000): n Improvement on Shimada **Public-key** Cryptosystem, Tamkang ... Storing
Keys in a Single **Key** Access Control ... Y. P, (2002): n **IC Card** Based Remote ...
www.cs.ccu.edu.tw/~ccc/english/ profile/publish/3_Lj.htm - 32k - Cached - Similar pages

Xref: netcom.com talk.politics.crypto:8667 sci.crypt:31848 alt. ...
... to do a version with 2 sound **cards**, one for ... 139.130.4.6) /micros/pc/oak England:
src.doc.ic.ac.uk ... FOR THE MATHEMATICALLY ORIENTED - HOW A QUICK **PUBLIC
KEY** WORKS ...
ftp.funet.fi/pub/crypt/msdos/callsec.faq - 26k - Cached - Similar pages

h   g g e c   e ch   c   b c e   c   h

[DOC] <u>Sixth APT Standardization Program (ASTAP) Forum</u>
File Format: Microsoft Word 2000 - <u>View as HTML</u>
... of the **multiplicative** group Zp* of the integers **modulo** p. ... the TC and shared with
each signer's **public key** or physical constituent such as an **IC card**. ...
www.aptsec.org/astap/meetings/Forum2002/Sixth-ASTAP/
Documentation/paper/ASTAP02-FR06-EG.IS-07.doc - <u>Similar pages</u>

<u>Implementation</u>
... Julio Lopez and R. Dahab, Technical report, **IC**-98-39 ... n), CH.Lim and HS.Hwang,
Public Key Cryptography 2000 ... Paar, Presented at the Fourth Smart **Card** Research
and ...
www.securitytechnet.com/crypto/ algorithm/implementation.html - 30k - <u>Cached</u> -
<u>Similar pages</u>

<u>◀</u> Goooooooooogle <u>▶</u>

Result Page: **Previous** <u>1</u> 2 <u>3</u> <u>4</u> <u>5</u> <u>6</u> <u>7</u> <u>8</u> <u>9</u> <u>10</u><u>11</u>   **Next**

| IC card and public key and modu | Search |

<u>Search within results</u> | <u>Language Tools</u> | <u>Search Tips</u>

<u>Google Home</u> - <u>Advertising Programs</u> - <u>Business Solutions</u> - <u>About Google</u>

©2004 Google

h　　　　g　g e c　　e ch　　　c　　　　　b c　e　　　　　　　　c　　　h